REMARKS

Applicants respectfully thank the Examiner for accepting the drawings filed on November 29, 2000. Claims 1, 3-4, and 6-26 are pending in the present case. Claims 1, and 6-26 are amended herein. Claims 2 and 5 are cancelled herein. Applicant respectfully requests reconsideration in view of the above amendments to the present application, and the arguments set forth below. No new matter is added herein.

CLAIM REJECTIONS

35 USC 102

Claims 10 and 17-18 are rejected under 35 USC 102(e) as anticipated by US Application Publication No. US 2001/0011308 by Clark, et al. (hereinafter Clark). Applicants have reviewed the Clark reference and respectfully asserts that it does not teach or suggest the embodiments of the present invention recited in Claims 10-12 and 17-18 for the following rationale.

As Applicants understand the reference, Clark teaches "[a] handheld computer which synchronizes with a host computer that has a display screen that is preferably an LCD. Clark at 1, ¶ 0009. However, Applicants find no teaching or suggestion within Clark directed towards enabling decryption of encrypted data from the handheld computer provided the identity of the handheld computer is authorized and disabling decryption if the identity is not authorized, as claimed. The computer taught by Clark differs from embodiments of the present invention recited in independent Claim 10.

As amended herein, independent Claim 10 reads as follows, with underlining added herein for emphasis:

10. A system for preventing unauthorized transfer of data between a portable computer system and a host system, comprising:

a) a portable computer device capable of synchronizing with said host;

b) an interface device compatible to receive said portable computer device and coupled with said host system and capable of facilitating communication between said portable computer device and said host system;

c) an identification authenticating component incorporated into one of said devices and providing a unique identification signal corresponding to the unique identity thereof; and

d) an identification authorizing component capable of determining if said unique identity is authorized for synchronization and for correspondingly enabling and disabling synchronization between said portable computer and said host system, wherein decryption of encrypted data from said portable computer device is enabled provided said unique identity is authorized and wherein said decryption is disabled if said unique identity is not authorized.

As amended herein, independent Claim 10 recites that decryption of encrypted data from a portable computer is enabled, provided that the portable computer's unique identity is authorized and that decryption is disabled if the unique identity is not authorized. This has advantages relating to data security including deterring transfer of encrypted data to unauthorized devices.

Clark does not teach enabling decryption of encrypted data from a portable computer provided the portable computer's unique identity is authorized and disabling such decryption where the unique identifier is not authorized, as recited in Claim 10 herein. Thus, Applicants respectfully assert that Clark does not anticipate Claim 10 and its dependent Claims 11-20. In fact, Clark teaches, instead, that:

> When the handheld computer is in the cradle and actively connected to the host computer, the handheld computer enters a mode where it *automatically captures* updated data in the host computer which is also contained in the handheld computer.

Id. at 2, ¶ 0011; italics added for emphasis. Moreover, Clark expressly teaches that "*synchronization is automatically performed* between the handheld computer system and the host computer to allow the user to have the most updated data." Id. at ¶ 16; italics added for emphasis.

Applicants respectfully suggest that such data may in fact include encrypted data. Further, Applicants respectfully point out that the automatic data exchange taught by Clark, which may include such encrypted data, is not enabled or disabled based on whether the handheld computer's unique identity is respectively authorized or not authorized.

Applicants respectfully assert that, in expressly teaching that synchronization and data capture is performed automatically when the handheld computer is cradled and actively connected to the host computer, Clark effectively teaches away from enabling decryption of encrypted data from a portable computer provided the portable computer's unique identity is authorized and disabling such decryption where the unique identifier is not authorized, as recited in Claim 10 herein. Applicants respectfully assert therefore that Clark does not teach or suggest the embodiments of the present invention recited in Claim 10.

35 USC 103

Claims 1, 8-9, 13, and 19-20

Claims 1, 8-9, 13, and 19-20 are rejected under 35 USC 103(a) over Clark in view of US Patent No. 5,887,063 to Varadharajan, et al. (hereinafter

Varadharajan). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claims 1, 8-9, 13, and 19-20 for the following rationale.

Claims 8-9 depend on Claim 1. Claims 13 and 19-20 depend on Claim 10. As discussed above, Clark does not teach or suggest and, in fact, teaches away from enabling decryption of encrypted data from a portable computer provided the portable computer's unique identity is authorized and disabling such decryption where the unique identifier is not authorized, as recited in Claims 1 and 10 herein. As Applicants understand the reference, Varadharajan teaches a communication system having a host device and a portable device intercommunicating via a communications medium, remotely or directly. Varadharajan, Col. 2, ll. 30-34. The teachings of Clark and Varadharajan, separately or combined, differ from the embodiments of the present invention recited in Claim 1 and 10.

As amended herein, independent Claim 1 reads as follows, with underlining added herein for emphasis:

> 1. A method for preventing unauthorized transfer of data between a portable computer system and systems of data storage and communication including an other computer, said method comprising:
>
> a) automatically receiving identification authentication information for said portable computer system by transferring identification authentication information between a portable computer system and a communication interface device, wherein said authentication information comprises a unique identity for said portable computer wherein said portable computer comprises a palmtop computer and said interface device comprises a palmtop computer system cradle;
>
> b) comparing said identification authentication information with a list of authorized portable computer system identities;

c) determining whether said portable computer system identity is authorized based on said identification authentication information and said unique identity;

d) enabling communication between said portable computer system and said other computer provided said identity is authorized and disabling said communication if said identity is not authorized; and

e.) enabling decryption of encrypted data from said portable computer system provided said identity is authorized and disabling decryption if said identity is not authorized.

As amended herein, Claim 1 recites a method that prevents unauthorized data transfer a palmtop computer and data storage and communication systems, such as another computer.

The method includes receiving identification authentication information for the palmtop computer by transferring identification authentication information, which includes a unique identity for the palmtop computer, between the palmtop computer and cradle interface device. The method further includes enabling communication between the palmtop computer system and the other computer, provided its identity is authorized and disabling such communication if its identity is not authorized.

Thus, communications between the palmtop computer and the data storage and communications systems through the docking cradle can be authorized or disabled, based on the identity of the portable computer, respectively whether authorized or not. This has advantages related to data, communication, and computer security, including respectively allowing or disabling direct (e.g., rather than remote) access between host and portable computer systems.

As Applicants further understand the Varadharajan reference, the communication system taught therein has "direct communications means for providing relatively secure and/or direct communications between" the host and the portable device. Id. at ll. 35-37, underlining added for emphasis. However, while Varadharajan further teaches that, while means detect when the portable device is docked with a cradle or support means (Id. at Col. 3, ll. 7-9), nevertheless no means are taught or suggested therein for detecting the unique identity of the docked portable device. Instead, Varadharajan expressly teaches that "[t]he host device preferably [i.e., not necessarily] includes means for identifying a request for *remote access* via [the] communication medium from a portable device and allowing access only on receipt from the portable device of [a] security key or code data or other data authenticating the identity thereof." Id. at ll. 15-20.

Notwithstanding whatever "relative" security and/or directness provided by the direct communications means taught by Varadharajan, Applicants respectfully assert that the reference fails to teach receiving identification authentication information for a palmtop computer by transferring identification authentication information, which includes a unique identity for the palmtop computer, between the palmtop computer and cradle interface device, as recited in Claim 1 herein. Applicants also respectfully assert that the reference fails to teach enabling communication between the palmtop computer system and the other computer, provided its identity is authorized and disabling such communication if its identity is not authorized, as recited in Claim 1 herein.

Further, Applicants respectfully assert that, in expressly teaching that "[t]he host device preferably includes means for identifying a request for *remote access* via [the] communication medium from a portable device and allowing access only on receipt from the portable device of [a] security key or code data or other data authenticating the identity thereof" (Id.), Varadharajan effectively teaches away from the embodiments recited in Claims 1 and 10 herein, which authorize or disable direct (e.g., rather than remote) access, via the docking cradle. Clark does not cure these defects of Varadharajan. Varadharajan does not cure the defects of Clark, discussed above. Further, Applicants find no teaching, suggestion or motivation in either Clark or Varadharajan to combine or modify their teachings to achieve the embodiments recited in Claim 1 herein.

Applicants respectfully point out that, obviousness can only be established by combining or modifying the teachings of the references cited to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found in either the references themselves or knowledge generally available to one of ordinary skill in the art. MPEP § 2143.01; In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

In as much as Clark and Varadharajan both teach away from embodiments recited in Claim 1 and lack any teaching, suggestion, or motivation to combine or modify their teachings to achieve such embodiments, Applicants respectfully assert that Clark and Varadharajan, separately or in combination, do not teach or suggest the embodiments recited in Claims 1, 8-9, 13, and 19-20, and in fact teach away therefrom.

Claims 2-6 and 21-22

Claims 2-6 and 21-22 are rejected under 35 USC 103(a) over Clark in view of Varadharajan, further in view of US Patent No. 5,600,800 to Kikinis, et al.

(hereinafter Kikinis). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claims 3-4, 6, and 21-22 for the following rationale.

As discussed above, Clark and Varadharajan, separately or in combination, do not teach or suggest the embodiments recited in Claim 1, and in fact teach away therefrom. Claims 3-4 and 6 depend on Claim 1. As Applicants understand the reference, Kikinis teaches transfer of identification data based on querying a user for authorizing passwords. Kikinis, Col. 12, ll. 1-6. However, Applicants find no teaching or suggestion to automatically transfer identity information, as recited in Claims 1 and 21 herein.

Further, Applicants respectfully assert that, in expressly teaching querying and use of passwords, Kikinis effectively teaches away from the embodiments of the present invention recited in Claims 1 and 21. Clark and Varadharajan do not cure these defects of Kikinis. Kikinis does not cure the defects in Clark and Varadharajan discussed above. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claims 2, 6, and 21-21 herein, and in fact, teach away therefrom.

Claim 7

Claim 7 is rejected under 35 USC 103(a) over Clark in view of Varadharajan, further in view of US Patent No. 6,157,825 to Frederick (hereinafter Frederick). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claim 7 for the following rationale. Claim 7 depends on Claim 1.

As discussed above, Clark and Varadharajan, separately or in combination, do not teach or suggest the embodiments recited in Claim 1, and in fact teach away therefrom. Claim 7 depends on Claim 1. As Applicants understand the reference, Frederick expressly "relates to wireless subscriber systems." Frederick, Col. 1, l. 10. However, Applicants find no teaching or suggestion therein directed to a method that prevents unauthorized data transfer a palmtop computer and data storage and communication systems (e.g., another computer), as recited in Claim 1 herein.

Further, Applicants respectfully assert that, in expressly teaching "granting or denying access to [a] wireless subscriber system," Frederick effectively teaches away from the embodiments of the present invention recited in Claims 1 and 7. Clark and Varadharajan do not cure these defects of Frederick. Frederick does not cure the defects in Clark and Varadharajan discussed above. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 7 herein, and in fact, teach away therefrom.

Claim 14

Claim 14 is rejected under 35 USC 103(a) over Clark in view of US Patent No. 4,593,353 to Pickholtz (hereinafter Pickholtz). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claim 14 for the following rationale.

As discussed above, Clark does not teach or suggest the embodiments recited in Claim 10, and in fact teaches away therefrom. Claim 14 depends on Claim 10. As Applicants understand the reference, Pickholtz teaches a computer software protection system. Pickholtz, Col. 2, l. 26. Applicants also understand

Pickholtz to expressly teach "first and second authorization codes .... recorded on a magnetic disc or other storage medium carrying proprietary software that is to be implemented in only an authorized data processing system[, which are] read prior to program execution." Id. at ll. 27-31.

Further, Pickholtz teaches that the first code is an encryption key to a pseudorandom generator provided in a hardware module connected in circuit with the data processing system, which generates a pseudorandom number by an algorithm unique to the authorized data processing system. This number is compared with the second authorization code to enable the software to execute, upon a favorable comparison. Id. at ll. 32-42.

However, Applicants find no teaching or suggestion therein directed to a system for preventing unauthorized transfer of data between a portable computer system and a host system, as recited in Claim 10 herein. Further, Applicants respectfully assert that, in expressly teaching first and second authorization codes, generation by a unique algorithm of a pseudorandom number enabled by the first code, which is an encryption key, and comparison of same to the second code, Pickholtz effectively teaches away from the embodiments recited in Claims 10 and 14 herein.

Clark does not cure these defects of Frederick. Frederick does not cure the defects in Clark, discussed above. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 14 herein, and in fact, teach away therefrom.

Claim 15

Claim 15 is rejected under 35 USC 103(a) over Clark in view of US Patent No. 5,239,166 to Graves (hereinafter Graves). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claim 15 for the following rationale.

As discussed above, Clark does not teach or suggest the embodiments recited in Claim 10, and in fact teaches away therefrom. Claim 15 depends on Claim 10. As Applicants understand the reference, Graves teaches a:

> system ... of [sic] providing information and services to a population of persons through portable devices which can be used to access any of a number of terminals to make use of the services offered at [the] terminals[, which,] in particular, provide for security against unauthorized access. The invention has use in the fields of automatic banking, automatic credit and debit transactions, passport and travel visa verification, health and medical records, security access, licensing, and any other like field where fraud may pose a problem.

Graves, Col. 1, lines10-21. Applicants also understand Graves to teach that "the system is comprised of a portable device such as a card [in contrast to a palmtop computer]" and "a peripheral device [e.g., in contrast to a host] such as a terminal." Id. at Col. 2, ll. 33-35, underlining added for emphasis.

Applicants further understand Graves to teach that "[t]he terminal contains ... a card reading device and a fingerprint scanner." Id. at ll. 43. The card has previously recorded fingerprint data, which is compared to the fingerprint scanned by the fingerprint scanner to authorize the transaction. Id. at ll. 50-54. Graves goes on to teach that other physical characteristics, such as "retinal or DNA scan" can possibly be applied as well. Id. at 54-59.

However, Applicants find no teaching or suggestion therein directed to a system for preventing unauthorized transfer of data between a portable computer system and a host system, as recited in Claim 10 herein. Further, Applicants respectfully assert that, in expressly teaching (1) that its usefulness lies in fields fraught with fraud problems, (2) that the portable device is a card, (3) to be read by a peripheral terminal, and (4) that to enable a transaction, a fingerprint (or other physical, biological characteristic) of the user must be scanned by the peripheral terminal, Graves effectively teaches away from the embodiments recited in Claims 10 and 15 herein.

Clark does not cure these defects of Graves. Graves does not cure the defects in Clark, discussed above. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 15 herein, and in fact, teach away therefrom.

Claim 16

Claim 16 is rejected under 35 USC 103(a) over Clark in view of Varadharajan, further in view of US Patent No. 6,480,101 to Kelly, et al. (hereinafter Kelly). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claim 16 for the following rationale.

As discussed above, Clark and Varadharajan, separately or in combination, do not teach or suggest the embodiments recited in Claim 10, and in fact teach away therefrom. Claim 16 depends on Claim 10. As Applicants understand the reference, Kelly expressly teaches enhancing performance of contactless proximity automated data collection systems, "which include a Tag, a Target, and a Host." Kelly, Col. 2, ll. 30-37.

Applicants further understand the reference to teach that "[t]he Tag is a portable thin card carried by an individual[, t]he Target is a radio frequency source that provides a link between the Tag and the Host controller." Id. at 38-40. However, Applicants find no teaching or suggestion therein directed to a system as recited in Claim 10 herein.

Further, Applicants respectfully assert that, in expressly teaching a portable thin card carried by an individual and an RF source that links between the card and a host controller, Kelly effectively teaches away from the embodiments of the present invention recited in Claims 10 and 16. Clark and Varadharajan do not cure these defects of Kelly. Kelly does not cure the defects in Clark and Varadharajan discussed above. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 16 herein, and in fact, teach away therefrom.

Claims 23 and 25

Claims 23 and 25 are rejected under 35 USC 103(a) over Clark in view of Kikinis. Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claims 23 and 25 for the following rationale.

Claim 23 is amended herein to read as follows, with underlining added herein for emphasis:

23. A communication system comprising:

a host computer system comprising a communication port;

a portable electronic device comprising a communication port and an identity reference; and

a communication module for coupling between said communication ports of said portable electronic device and said host computer system, said communication interface module comprising:

an authentication device for authenticating said identity reference; and

a communication interface circuit coupled to said authentication device and for allowing direct communication between said portable electronic device and said host computer system provided said authentication device indicates a proper authentication of said identity reference and, otherwise, for disallowing communication between said portable electronic device and said host computer system, wherein decryption of encrypted data from said portable computer device is enabled provided said unique identity is authorized and wherein said decryption is disabled if said unique identity is not authorized.

As discussed above, Clark and Kikinis, separately or in combination, do not teach or suggest the embodiments, such as those recited in Claim 23, and in fact teach away therefrom. Claim 25 depends on Claim 23. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 23 and 25 herein, and in fact, teach away therefrom.

Claim 24

Claim 24 is rejected under 35 USC 103(a) over Clark in view of Kikinis and further in view of Varadharajan. Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claim 24 for the following rationale.

As discussed above, Clark, Kikinis, and Varadharajan separately or in combination, do not teach or suggest the embodiments, such as those recited in Claim 23, and in fact teach away therefrom. Claim 24 depends on Claim 23. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 24 herein, and in fact, teach away therefrom.

Claim 26

Claim 26 is rejected under 35 USC 103(a) over Clark in view of Kikinis, further in view of US Patent No. 6,286,099 to Kramer, et al. (hereinafter Kramer). Applicants have reviewed the references cited and respectfully assert that they do not teach or suggest the embodiments of the present invention recited in Claim 26 for the following rationale.

As discussed above, Clark and Kikinis separately or in combination, do not teach or suggest the embodiments, such as those recited in Claim 23, and in fact teach away therefrom. Claim 26 depends on Claim 23. As, Applicants understand the reference, Kramer expressly states that its teaching:

> relates to secure, electronic *payment in exchange for goods and services purchased over a communication network*, and more specifically, to determining the security properties of the hardware devices and accompanying software used in the payment network, *for the purpose of allowing financial institutions to allow or disallow specific types of transactions* based on the security characteristics of the device. A preferred embodiment of the invention facilitates public key cryptography for securely transmitting transactions *over a public communications network* in a manner that is independent of any specific financial institution is provided [sic].

Kramer, Col. 1, ll. 6-19, italics added for emphasis. Applicants further understand Kramer to expressly teach that its "invention provides for determining point of interaction device security properties for secure transmission of a transaction ... over a public communication system, such as the Internet." Id. at Col 2, ll. 60-66, underlining added for emphasis.

However, Applicants find no teaching or suggestion in the Kramer reference directed to allowing direct communication (e.g., in contrast to communication over Kramer's public communications network), as recited in Claim 23 herein. Further, Applicants respectfully assert that Kramer's teachings directed towards financial transactions, for financial institutions, and over public communications networks such as the Internet expressly teach away from embodiments recited in Claims 23 and 26 herein.

Clark and Kikinis do not cure these defects of Kramer. Kramer does not cure the defects of Clark and/or Kikinis. Thus, Applicants respectfully assert that these references, combined or separately do not suggest the embodiments recited in Claim 26 herein, and in fact, teach away therefrom.

CONCLUSION

By the rationale stated above, Applicants respectfully assert that Claims 1, 3-4, and 6-26 are allowable under 35 USC §§ 102(e) and 103(a). Accordingly, Applicants respectfully request that the rejection of these claims under these statutes be withdrawn and that Claims 1, 3-4, and 6-26 be timely allowed.

Please charge our deposit account No. 23-0085, for any unpaid fees.

Respectfully submitted,

WAGNER, MURABITO & HAO, LLP

Dated: Aug. 20, 2004

Lawrence R. Goerke
Reg. No. 45,927

WAGNER, MURABITO & HAO, LLP
Two North Market Street, Third Floor
San Jose, CA 95113

Tel.: (408) 938-9060
Fax: (408) 938-9069